Part 1

Exchange Fundamentals

- Chapter 1: Introducing Exchange Server 2010
- Chapter 2: Introduction to Email Administration
- Chapter 3: Standards and Protocols
- Chapter 4: Understanding Availability, Recovery, and Compliance
- Chapter 5: Message Security and Hygiene
- Chapter 6: Introduction to PowerShell and the Exchange Management Shell
- Chapter 7: Exchange Autodiscover
- Chapter 8: Virtualizing Exchange Server 2010
- Chapter 9: Exchange Server, Email, and SharePoint 2007

Chapter 1

Introducing Exchange Server 2010

Email clients used to be fairly simple and text based. Email servers had few connectivity options, no high-availability features, and no integrated directory. Then, beginning in the mid-1990s we saw a big push toward providing email service to most of our user communities. We also saw email go from an occasionally used convenience to a business-critical tool. Business management and users demanded more features, better availability, and more connectivity options as the email client and server evolved.

Microsoft released Exchange Server 4.0 (the first version of Exchange Server) in 1996 and the product has been evolving ever since. Exchange Server 2010 is the fifth major release of the Exchange Server family and represents a significant evolution of the product. The features and functions of this new release include not only feature requests from many thousands of Microsoft's customers, but also requirements shared internally at Microsoft by Microsoft Consulting Services and their own IT department, which supports nearly 100,000 mailboxes.

When we started planning this chapter, we considered discussing exclusively what was new in Exchange Server 2010 since the release of Exchange Server 2007. However, as of this writing most Exchange Server customers are still using Exchange Server 2003 rather than Exchange Server 2007. For this reason, we want to incorporate into this chapter a summary of the changes that have been made to Exchange Server since Exchange Server 2003.

In this chapter, you will learn to:

- Understand new high-availability options
- Understand new recipient management features
- Recognize Exchange architecture changes

Getting to Know Exchange Server 2010

It seems that we approach any new release of Exchange Server with a sense of both excitement and trepidation. We look forward to the new features and capabilities that are introduced with a newer version of a product. Certainly features such as the Exchange Management Shell, new database replication technology, antispam, resource management, and security features will allow us to deliver better, more reliable messaging services to our end users.

On the other side of the coin is the feeling that there is a whole new series of features that we have to learn inside and out so that we can better use them. Sure, we know Exchange

2003 or Exchange 2007 pretty well, but there will be new details to learn with Exchange 2010. Sometimes these implementation or management details are things that we have to learn the hard way — thus the trepidation associated with any new version of Exchange.

However, this next milestone in the evolution of Exchange Server is a good one. We can't help but be excited about learning about this new version and sharing what we have learned. We hope that you will feel the same sense of excitement. We have picked a top-ten list of new features that we like and hope that you will investigate further as you start to learn Exchange Server 2010. Some of these are summarized in this chapter while most of these you will find in more detail in later chapters. The new features are as follows:

- Powerful message transport rules applied and enforced at the server
- Continuously replicated Exchange databases and failover to a replicated database at the database level rather than the server level
- MAPI clients now able to communicate with the Client Access server rather than directly with the database engine
- Vastly improved antispam features
- Customizable ''over quota,'' nondelivery messages, and end-user informational messages
- Exchange Management Shell command-line and scripting interface
- Improved calendaring support via calendar concierge, the Availability service, and resource mailboxes
- Message routing now based on Active Directory site rather than Exchange administrator–configured routing groups
- Unified messaging technology that is now an integrated part of Exchange Server 2010
- Completely rewritten and vastly improved Outlook Web App (formerly known as Outlook Web Access)

This list could go on for the entire chapter, but this gives you a taste of a few of the features that excite Exchange administrators as well as administrators from other messaging systems when they talk about Exchange 2010.

Learn the Exchange Management Shell (and Wear Sunscreen!)

To those of you who have been around the Internet long enough to remember the ''Wear Sunscreen'' email that was supposedly the 1997 commencement address to MIT given by Kurt Vonnegut but was in reality a column written by the *Chicago Sun Tribune*'s Mary Schmich, I give you ''Learn the Management Shell'':

- If we could offer you one important tip when learning Exchange Server 2010, it would be that you should get to know the Exchange Management Shell (EMS). Sure, it looks intimidating and nearly everything you will ever need to do is in the Exchange Management Console. Many Exchange gurus will back us up on the value and usefulness of the new EMS, whereas they might not agree with us on things such as using real-time block lists, making full backups daily, and keeping lots of free disk space available.
- Make regular Exchange data backups.

- Document.
- Don't believe everything you read from a vendor; their job is to sell you things.
- Don't put off maintenance that might affect your up-time.
- If you get in trouble, call for help sooner rather than later. A few hundred dollars for a phone call to your vendor or Microsoft Product Support Services is better than a few days of downtime.
- Share your knowledge and configuration information with coworkers.
- Accept certain inalienable truths: disks will fail, servers will crash, users will complain, viruses will spread, and important messages will sometimes get caught in the spam filter.
- Get to know your users and communicate with them.
- SharePoint provides a good alternative for sharing many types of data you might find in public folders; get to know it.
- Make regular backups of your Active Directory.
- If a consultant is telling you something that you know in your gut is wrong, double-check his work or run his recommendation by another colleague. Second opinions and another set of eyes are almost always helpful.
- Be careful with RegEdit, Active Directory Service Interfaces Editor (ADSI Edit), and any advice you read on the Internet (or in books).

But trust us on the EMS.

In this chapter, we will cover the changes to Exchange 2010 not only to give experienced Exchange administrators the proper perspective on Exchange 2010, but also to educate newly minted Exchange administrators on just how powerful Exchange has become.

Exchange Server Architecture

Since Exchange Server 2003, a number of significant changes have been made to the architecture of Exchange Server. These changes positively improve the performance and scalability of Exchange Server, but they also make some pretty significant changes in the platform on which you support Exchange Server.

x64 Processor Requirement

For a long time, one of the most discussed (and perhaps the most controversial) enhancement to Exchange 2007 (and now Exchange Server 2010) was that Exchange 2007 Server used 64-bit extensions. That meant your production servers would have to have x64 architecture–based Intel Xeon and Pentium processes or AMD64 architecture–based AMD Opteron and Athlon processors. There was an x86 build of Exchange Server 2007 that could be used for evaluation, classroom, or lab purposes, but not in production. There is only an x64 build of Exchange Server 2010.

Although many people are thrilled with this change in the architecture, there are, no doubt, folks screaming, ''What? I have to buy new hardware just to upgrade?'' A good response to this concern is that on most messaging system upgrades, the hardware is usually replaced anyway.

Certainly this is true for hardware that has been in production for more than three or four years. Add to this the fact that there is no ''in-place'' upgrade from Exchange 2000, 2003, or 2007 to Exchange Server 2010.

The good news is that most server-class hardware that has been purchased since the end of 2005 or later probably already includes the x64 processor extensions that Windows 2008 x64 requires. If you have existing hardware you want to use with Exchange 2010, confirm with your vendor that it will run Windows 2008 x64.

Is the decision to move to the x64 memory architecture a bold move? Is the Exchange team forging the way to more robust applications? Well, to a certain degree, yes, but the move to the 64-bit architecture is more out of need than the desire to forge a bold, modern path. Anyone who has supported an older version of Exchange Server with a large number of mailboxes knows that Exchange is constrained by the amount of RAM that it can access and that Exchange significantly taxes the disk I/O system. Further, as Exchange Server scaled to support more connections, limitations in the x86 operating system kernel also began to surface.

The number one reason that the x64 processor extensions are required is to provide Exchange Server with access to more than just a few gigabytes of RAM. With more RAM available, Exchange caching is more efficient and thus reduces the I/O requirements that are placed on the disk subsystem. More RAM also helps provide the improved scalability and features that organizations require, such as improved high availability, larger mailboxes, messaging records management features, improved message content security, transport rules, unified messaging integration, and improved journaling. The bottom line: the x64 instruction set for processors means more RAM for applications.

If you are not sure whether your existing hardware supports the x64 extensions, you can check in a number of ways. One approach is to check with the hardware vendor regarding x64 for your server hardware. Another way, if the computer is already running Windows, is to get a handy little program called CPU-Z from `www.cpuid.com`. Figure 1.1 shows the CPU-Z program.

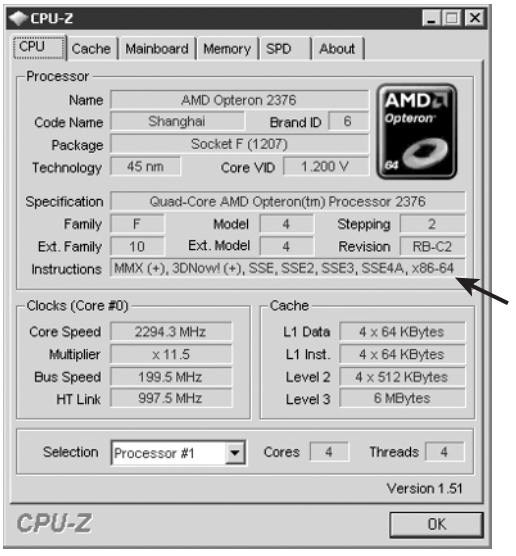


FIGURE 1.1
Using CPU-Z to identify the CPU type

Notice in the Instructions line of CPU-Z that this particular chip supports x86-64. This means this chip will support the x64 instruction sets. Intel chips will report that they support the EM64T instruction set.

Windows Server 2008 x64

Because of some of the underlying requirements of Exchange Server 2010, you must run Windows Server 2008 x64 Service Pack 2 or Windows Server 2008 R2. Although many people are comfortable with Windows Server 2003, that operating system is fairly dated and does not have some of the components necessary for Exchange Server 2010. The following two editions of Windows 2008 will support Exchange Server 2010:

- Windows Server 2008 Standard x64 SP2 or R2
- Windows Server 2008 Enterprise x64 SP2 or R2

The Exchange Server 2010 management tools will run on the x64 version of Windows Vista Ultimate, Enterprise, and Business as well as Windows 7.

Installer, Service Pack, and Patching Improvements

The setup process in Exchange 2000/2003 had some serious annoyances; actually the whole process of getting a server up and running was pretty annoying. If a server did not meet the prerequisites, you had to close the Setup program, fix the problem, and then restart Setup. Once you got the release to manufacturing (RTM) or ''gold'' version installed, you had to install the most recent version of the Exchange service pack. Finally, you had to research all the post-service pack–critical fixes and apply them (sometimes in a specific order).

Microsoft has improved the setup process for Exchange Server 2010 as well as simplified patching. These improvements have been made in four key areas:

- The Exchange Server 2010 Setup program is good at finding missing prerequisites, letting you fix the missing prerequisite and then continue without starting over (unless a reboot is required after installing a prerequisite).
- The entire setup process can be performed from the command line using the `setup.com` program and EMS cmdlets.
- Service packs are now released as a complete installation pack; all updates are built into the service pack and you can install directly from the latest service pack. That means no more installing the RTM version and then applying the latest service pack.
- Rollup releases are now released approximately once every two months and contain a cumulative set of patches and critical fixes since the last service pack. So, rollup fix 4 (RU4) will contain all the updates contained in RU3 plus the other fixes released since RU3 was released.

Now all you have to do to get an Exchange Server completely built is to download the latest service pack, install Exchange Server 2010 from the latest service pack binaries, and then download the latest Exchange Server rollup fix and apply that fix. You can even simplify this process a bit more if you download the latest rollup fix MSP file and then copy it to the `Exchange 2010 setup \Updates` folder. Doing so greatly simplifies getting a server up and running as well as properly patched.

APPLYING SPECIAL HOTFIXES

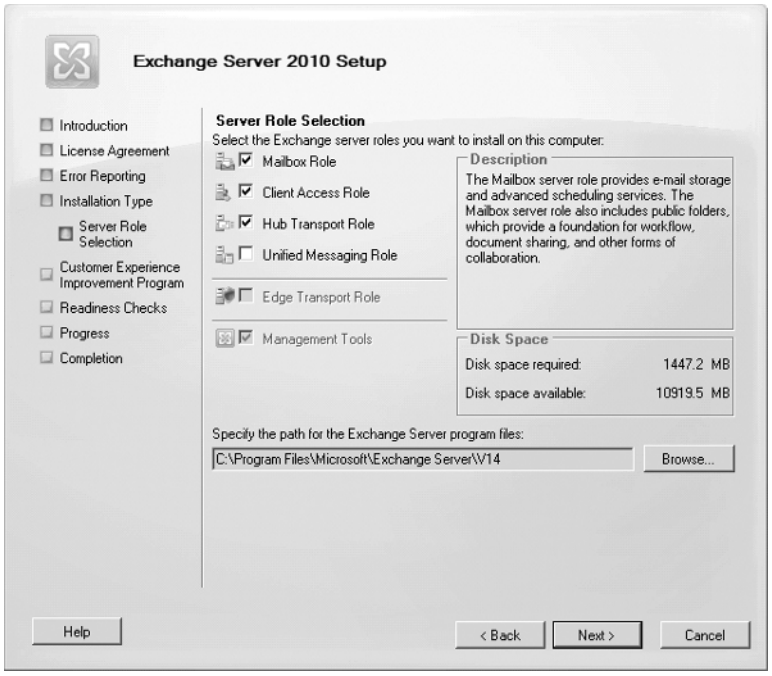
If you get a rollup fix such as Exchange 2010 rollup fix 4 and then later you require an individual hotfix from Microsoft to address a specific issue, you may need to uninstall the post–rollup 4 hotfix prior to installing rollup fix 5. If you ever get a hotfix for Exchange 2010 to address a specific issue, always ask the Microsoft product support person if you will have to uninstall it prior to applying the next rollup.

Server Roles

In earlier versions of Exchange, once the Windows server was prepared to support Exchange, you simply installed an Exchange server. Then you customized the Exchange configuration, configured Internet Information Server (IIS), disabled unnecessary services, and prepared the server to assume the role you wanted it to assume, such as a Mailbox server, a bridgehead server, an Outlook Web Access front-end server, and so on.

Exchange 2007 officially introduced the concept of server roles at the point of setup; this continues with Exchange Server 2010. During the installation process, the Setup program (Figure 1.2) asks the installer which roles the server will be performing.

FIGURE 1.2
Specifying server roles



When running Setup, if you choose a custom installation, during setup you can specify the server roles by choosing from among the options in Table 1.1.

Once a role is selected, only the components necessary for that role are installed. This reduces the overhead on machines that are dedicated to a particular task (such as a Hub Transport server); ensures that no unnecessary executables, DLLs, or services are installed;

and makes creating dedicated server roles much easier. In a small organization with only one Exchange server, the same server may be assigned the Mailbox, Hub Transport, and Client Access server roles.

HIGH-AVAILABILITY DECISIONS

High-availability decisions do not need to be made at installation time. Unlike previous versions of Exchange Server, high availability for Exchange Server 2010 databases can be added incrementally *after* the initial deployment of the Mailbox server. There is no clustered mailbox server installation option.

TABLE 1.1: Server Roles

SERVER ROLE	PURPOSE
Mailbox role	Supports mailboxes and public folders.
Client Access role	Supports functions such as Outlook, Outlook Web App, Outlook Anywhere (RPC over HTTP), Windows Mobile ActiveSync, POP3, and IMAP4, and supports web services such as Autodiscover, the Availability service, and calendar sharing.
Hub Transport role	Supports message transport functions such as delivering mail locally (to other Exchange servers in the organization) or externally (to an SMTP smart host such as an Exchange Edge Transport server). Using transport rules, the Hub Transport or Edge Transport roles can also help enforce messaging policies.
Unified Messaging role	Supports delivery of inbound voicemail and Outlook Voice Access features.
Edge Transport role	Supports separate antispam and antivirus functions for inbound and outbound messaging. The Edge Transport server is installed on a stand-alone machine usually in a perimeter network.

Edge Transport Services

The amount of spam and viruses that some organizations receive is staggering. Even small organizations are receiving tens of thousands of pieces of spam, dozens of viruses, and hundreds of thousands of dictionary spamming attacks each week. Some organizations estimate that more than 90 percent of all inbound email is spam or other unwanted content. Keeping as much of this unwanted content away from your Exchange servers as possible is important. A common practice for messaging administrators is to employ additional layers of message hygiene and security. The first layer is usually some type of appliance or third-party SMTP software package that is installed in the organization's perimeter network. The problem with these third-party utilities is that the administrator has to become an expert on an additional technology.

Is the Edge Transport Server Role Required?

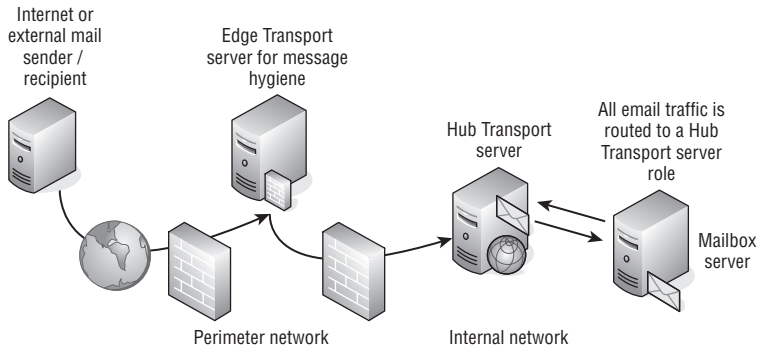
A common misconception about Exchange 2010 is that the Edge Transport role is required for Exchange 2010. This is not the case. Inbound email can be sent directly to the Hub Transport role, or you can continue to use your existing third-party antispam/message hygiene system to act as an inbound message relay for Exchange Server.

Microsoft's solution to this dilemma is the Edge Transport server. The Edge Transport server is a stand-alone message transport server that is managed using the EMS and the same basic management console that is used to manage Exchange 2010. A server functioning in an Edge Transport role should not be a member of the organization's internal Active Directory.

Functions such as transport rules are identical to those that run on an Exchange 2010 Hub Transport server. Content filtering (formerly referred to as the Intelligent Message Filter, or IMF) and Microsoft Forefront Security for Exchange are implemented on the Edge Transport server.

An example of how an organization might deploy an Edge Transport server is shown in Figure 1.3. Inbound email is first delivered to the Edge Transport servers that are located in the organization's perimeter network, where the message is inspected by the content filter, Forefront Security for Exchange, and any message transport rules. The inbound message is then sent on to the internal Hub Transport servers. Additionally, the Exchange 2007 Hub Transport servers are configured to deliver mail leaving the organization to the Edge Transport servers rather than configuring the Hub Transport servers to deliver mail directly to the Internet.

FIGURE 1.3
Deploying an Edge Transport server



The Edge Transport server is a fully functional SMTP message hygiene system with many of the same features that are found in expensive message hygiene software packages and appliances. The following features are included:

- Per-user safe-sender, safe recipient, and blocked sender lists are automatically replicated from the user's mailbox to the Edge Transport server. For organizations using Exchange 2007, this represents a nice set of improvements.
- Recipient filtering is enabled when valid recipients are synchronized to the Edge Transport server's local Active Directory Application Mode (ADAM) database.
- Sender and recipient filtering can be configured via administrator-controlled lists.

- Integrated Microsoft content filter is included for spam detection. Spam can be rejected, deleted, quarantined, or delivered to the user's Junk E-mail folder.
- Multiple message quarantines allow messages that are highly likely to be spam to be quarantined and sent to a quarantine mailbox on your Exchange server. A separate quarantine exists in the form of the user's Junk E-mail folder for messages that are still tagged as spam but with a lower Spam Confidence Level (SCL).
- Microsoft Forefront Security for Exchange Server (formerly known as Antigen) is available for the Edge Transport server when Enterprise client access licenses are used.
- Daily content filter and virus signature updates are available for organizations using Microsoft Forefront Security for Exchange Server.
- Real-time block lists (RBLs) and IP Reputation Service allow an IP address to be checked to see if it is a known source of spam. Reputation filters can be updated on a daily basis.
- Sender ID filters allow for the verification of the mail server that sent a message and whether it is allowed to send mail for the message sender.
- Sender reputation filters allow a sender to be temporarily placed on a block list based on characteristics of mail coming from that sender, such as message content, Sender ID verification, and sender behavior.

Unified Messaging

The concept of unified messaging means that information from multiple sources is accessed in a single location. This concept is by no means a new one; third-party vendors have had fax and voicemail gateways for most major email systems. The Exchange 2010 Unified Messaging server role represents Microsoft's entrance into this market. This can make users more efficient by providing a single location for inbound information; voicemails can be read via Outlook Web App, Outlook, or Windows Mobile 6.5 or later devices. In addition, missed call information (someone who calls but does not leave a voicemail message) is sent to the user's mailbox.

An example of a voicemail that has been delivered to a user is shown in Figure 1.4. The form you see in the figure is in Outlook Web App 2010 and includes a player control for playing the message via the PC speakers.

The message also includes the ability to play the voice message on your desk phone. The Play On Phone option allows you to instruct the Unified Messaging server to call you at a specified extension (or optionally an external phone if the Unified Messaging dial-plan allows).

Further, the user can call the Unified Messaging server via the telephone and listen to their voicemail, have their email read to them, listen to their calendar, rearrange appointments, or look up someone in the global address book. Unified Messaging also allows the administrator to build a customized auto-attendant for call routing. In our experience, a typical voicemail (using the default MP3 codec) takes between 2 KB and 3 KB per second of message time, but this amount can be changed. However, with higher-quality recordings come higher message sizes.

The Unified Messaging server role functions as just another Exchange server in your organization, but this role includes components that allow IP-based phone systems and IP/PBX (public branch exchange) gateways to interface directly with Exchange over the network. This can take place provided the IP phone system or IP/PBX can communicate using Session Initiation Protocol (SIP) over TCP or Real-Time Transport Protocol (RTP) for voice communication.

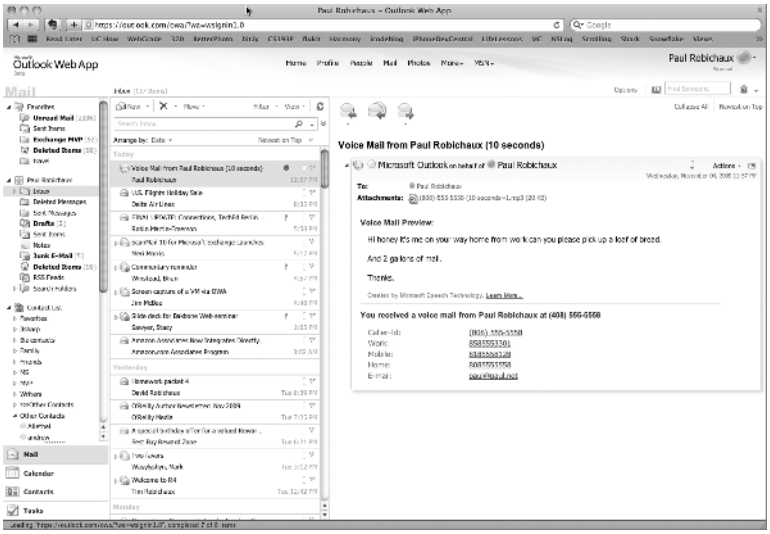


FIGURE 1.4
Viewing a voicemail message sent via Unified Messaging

Not all voice systems are going to support this feature ''right out of the box.'' More and more vendors (such as Cisco and Mitel) are tweaking their Voice over Internet Protocol (VoIP) systems to talk directly to Exchange Server 2010 Unified Messaging, but you may still require a VoIP gateway of some type. Many traditional ''hard-wired'' PBXs will require a PBX-to-VoIP gateway, but even some VoIP systems will require a VoIP-to-VoIP gateway.

If you are like us, you are more of a specialized network administrator. We have never managed a phone system in the past and are only slightly familiar with some of the phone terminology. We just assumed that VoIP was VoIP and that was that. Working with the folks who manage your telephone system will be a new and exciting experience. We were quite surprised to learn that there are more than 100 implementations of SIP on the market.

As of 2010, unified messaging solutions have only about a 10 to 15 percent market penetration — that is, of course, depending on whose survey you read and how you define unified messaging. Some vendors define it as delivering a voicemail to a user's computer and allowing them to play the voicemail over the PC speakers; this voicemail might have been delivered to the user's mailbox (on the server) or it might have been *pulled* by Outlook or another client application and stored in the user's PST file. Some vendors consider solely inbound faxing to be a unified messaging solution, though in our opinion that is not terribly unified.

EXCHANGE 2010 UNIFIED MESSAGING AND FAXING

The Exchange 2007 implementation of unified messaging implementation only supported inbound faxing. This feature has been removed from Exchange Server 2010. For a comprehensive faxing solution, we recommend you take a look at one of the many third-party faxing solutions. One of the reasons for this is that the Exchange 2007 solution only provided inbound faxing, but many third-party solutions on the market that integrate well with Exchange provide both inbound and outbound faxing.

Microsoft has decided to get into the unified messaging market for a number of reasons, including the fact that unified messaging has a fairly low market penetration thus far.

Customers are often reluctant to deploy unified messaging solutions due to the complexity, administrative overhead, schema changes, client-side deployment requirements, and cost. Microsoft is determined to make their unified messaging implementation less expensive than competing products and much better integrated with Active Directory.

When the Exchange 2010 Unified Messaging role is integrated with an IP-based phone system or a PBX with an IP/PBX gateway, the following additional functions may be possible:

- Inbound voicemail is delivered directly to the user's mailbox.
- Users can call in to the phone system to have their email read to them, to listen to their schedule, or to move appointments around on their schedule and notify attendees.
- Users can call in to the phone system to look up users from the Global Address List.

Unified Messaging Message Sizes

A typical voicemail uses the default MP3 between 2 KB and 3 KB per second of message time, but this amount can be changed. The Exchange Server 2010 Unified Messaging server supports the MP3, WMA, G.711 PCM, and GSM codecs. However, with higher-quality recordings come larger message sizes.

Improved High-Availability Features

One of the biggest enemies of high availability is slow restoration times. As mailbox databases get larger and larger, restore times get longer and longer. Often this is used as a rationale for limiting user's mailbox sizes to less than what they need to do their jobs effectively.

As mentioned earlier, when Microsoft released Exchange Server 2007, they introduced a new technology called continuous replication. This technology allowed Microsoft to introduce three new features to improve high availability: the Local Continuous Replication (LCR), Cluster Continuous Replication (CCR), and Standby Continuous Replication (SCR) features. These features allowed a database to be initially seeded with another copy and then the log files to be replicated in near real time and replayed to the copy of the database. The database copy could then be restored quickly (in the case of LCR) or brought online in the event of a server failure.

Exchange 2007 CCR leveraged Windows Failover Clustering so that in the event of a server failure the server could automatically be recovered. SCR was used so that even a single database failure could be recovered by being brought online (manually) on a remote Exchange server. CCR was designed as a high-availability solution, whereas SCR was designed to provide resiliency.

Exchange Server 2010 has taken the continuous replication and clustering technologies even further so that the lines between high availability and resiliency have been blurred. Windows Failover Clustering is now used much differently than it was in the past and the complexities of clustering are better hidden from the Exchange Server administrator. The Exchange 2010 high-availability technology is easy to incorporate with existing Exchange 2010 Mailbox servers. Individual databases can now be replicated to multiple servers, and failover can automatically occur, not at the server level but at the database level.

Exchange 2010 makes building a failover cluster so much simpler than with past versions that the technology will be easy to implement even for small organizations with no clustering expertise.

Continuous Replication Basics

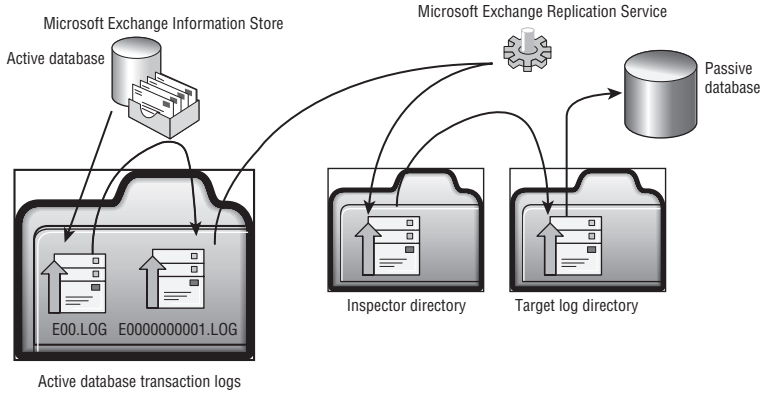
If we had to pick a single technology that is the most compelling in Exchange Server 2010, it would be the continuous replication technology. This new technology supports the ability to replicate a database to one or more additional Exchange Mailbox servers within your organization.

Unlike many tools from third-party vendors, which replicate data either at the disk block level or by taking snapshots of the disk and replicating changes, Exchange continuous replication is more similar to the SQL Server *log shipping* technology. This is considered similar to a *pull* model, but it is the active copy of the database that does the work. The replication service managing the passive copy of the database communicates with the active copy and indicates which logs the passive copy needs to keep the database in sync. The active source Exchange database, logs, and database engine do not even realize they are being copied. The Microsoft Exchange Replication Service (`Microsoft.Exchange.Cluster.ReplayService.exe`) handles copying the logs and managing the passive databases.

Initially (as when continuous replication is set up or reconfigured) the current copy of the database is copied to the passive location; this is called *seeding*. As an Exchange transaction log is filled up and renamed, (that is, when the `E00.LOG` file is filled and then renamed to `E000000001.LOG`), the renamed and closed log file is then copied to the passive location. The information store service then verifies the log file and commits it to the passive copy of the database. So the actual database file is not replicated at all, but it is kept in sync by copying the log files and replaying them.

You will probably understand this concept better with an illustration. Figure 1.5 shows an example of how this process works. The Exchange database engine is run by the Microsoft Exchange Information Store; transactions fill up the current transaction log (`E00.LOG`). The transaction log file (`E00.LOG`) is renamed to the next available transaction log filename (in this case `E0000000001.LOG`). All of this is handled by the Information Store service.

Figure 1.5
How continuous replication works



If continuous replication is enabled, the Microsoft Exchange Replication Service copies the `E0000000001.LOG` file to the Inspector directory. This folder exists on any server within the database availability group (DAG) that has a copy of the database.

The service performs an intensive verification of the log files in the Inspector directory to ensure they are not corrupted. Once the log files are verified as not being corrupted, they are

checked to ensure that they are in the correct sequence. Once this is verified, the replication service copies the log file (E0000000001.LOG) to the target log file directory. The Information Store service then replays the transactions found in the E0000000001.LOG file and the transactions are committed to the passive copy of the database.

At any given time, the most out-of-sync passive copy of the database will be approximately 15 minutes. The 15-minute lag time would be in a worst-case scenario such as in the dead of night when there is absolutely no activity on the mailbox database. During a normal workday in which users are actually using the database, the passive copy of the database will be no more than a few minutes behind.

If a database is dismounted or the Information Store service is stopped, the data is all committed to the active database and the log files are pulled over to the servers that hold a passive copy of the database. If the administrator has to manually switch over to the passive copy of the database, the passive copy should be completely synchronized with the active copy of the database.

Mailbox Database Mobility

Exchange 2010 introduces the concept of *database mobility*. Database mobility is a set of technologies and features that allow a mailbox database to be replicated to more than one Exchange server in an organization and that database to be brought online if the active copy of the database is no longer available. High availability is no longer tied to a specific server but rather to individual databases.

A mailbox database can be replicated to any Exchange 2010 Mailbox server within the same DAG. The DAG is a collection of one to 16 Exchange 2010 Mailbox servers that can be configured to host a set of databases. The DAG is the boundary of database replication and can span multiple Active Directory sites and geographic locations.

Figure 1.6 shows a simplified example of a DAG. This group has three Exchange Mailbox servers as members and each of the servers has a single ''active'' mailbox. The server in Tokyo has an active mailbox database called Executives, but a copy of this database is replicated to the Denver and Honolulu servers. The database can be replicated to one or more servers in the DAG.

In the event of a failure on the Tokyo Mailbox server or a problem with the Executives database on the Tokyo Mailbox server, the database on either the Denver or the Honolulu server will be made active and users will be redirected to the new ''active'' location.

Database mobility replaces the SCR, CCR, LCR, and single-copy cluster features that were available in previous versions of Exchange.

Real World Scenario

High Availability and Resiliency

XYZZY Corporation has their headquarters office in South Florida as well as regional offices on the East Coast and in Colorado. The Colorado office has a small data center. Most data services are handled in the Florida office. In recent years, the South Florida office has had several instances where they had to close the office and shut down their data center because of hurricanes. This means not only does the South Florida office lose Exchange services but it also loses all users in the eastern United States.

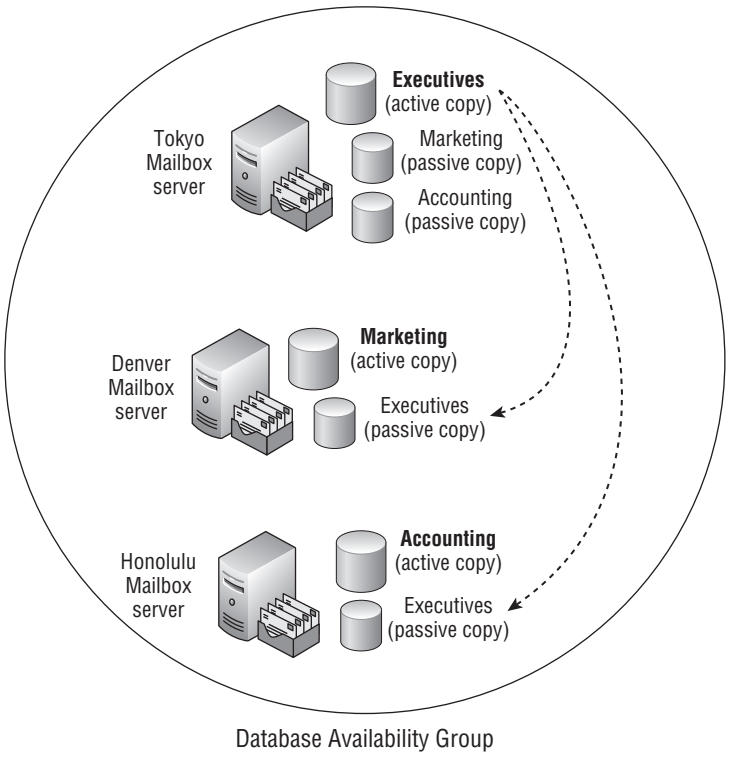
XYZZY requires a high-availability solution that not only provides email access in the event of an Exchange server failure in the local office, but also provides a contingency in case their headquarters office has to be shut down. Email should be hosted in the Colorado office in the event the Florida office has to be closed. The solution that switches active email services over to Colorado must be smooth and simple.

The company decided to implement Exchange Server 2010 database availability groups (DAGs). The Eastern US DAG has three Mailbox servers: two Mailbox servers are in South Florida and one in Colorado. The databases assigned to the two South Florida servers will first fail-over to one or the other of those servers. In the event that both servers in Florida must be shut down, the databases will be switched over to the Mailbox server in Colorado.

MAPI and Directory on the Middle Tier

Previously, in all versions of Outlook and Exchange Server, the Outlook client (using MAPI over RPC, not RPC over HTTP) had to be configured to connect to a specific Exchange server. A traditional MAPI client-to-Exchange configuration is shown in Figure 1.7. First, the Outlook MAPI client would connect to a process the Exchange server's System Attendant service runs to get a referral to a global catalog server (for the Global Address List) or possibly to handle directory lookups on behalf of the Outlook client.

FIGURE 1.6
Simple database availability group



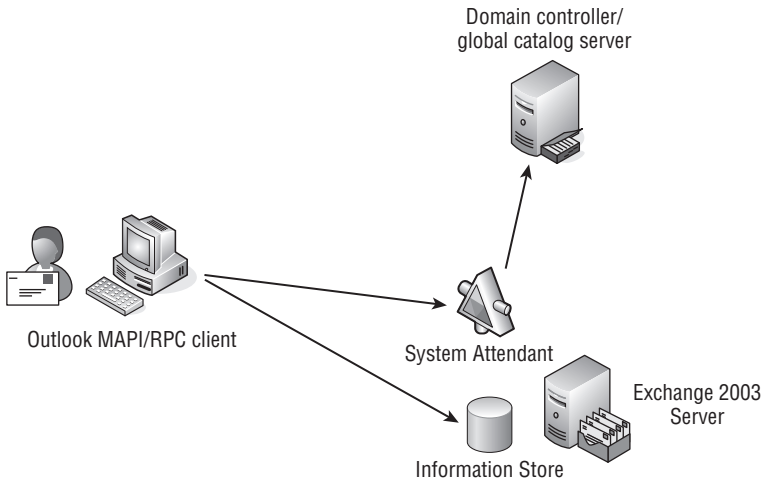


FIGURE 1.7
Traditional MAPI to Exchange connectivity

Second, the client connects to the RPC interface provided by the Information Store service (`store.exe`). This means that the Outlook RPC client is connected directly to the information store on the Exchange server on which their mailbox database resides.

Although this works just fine for earlier versions of Exchange Server, this makes building a version of Exchange that allows failover at the database level rather than the server level much more difficult. The Exchange developers had to find a new way to allow Outlook clients to connect both to their mailbox database and to the directory. Rewriting how Outlook works was not an option since Exchange 2010 has to be backward compatible with earlier versions of Outlook such as Outlook 2003 and 2007.

The solution is to ''abstract'' the MAPI interface out of the Mailbox server's System Attendant and Information Store services. Rather than having the Outlook MAPI client connect directly to the Mailbox server, the Outlook client connects to a service that proxies the connections to the server on which the active mailbox database currently resides. The mailbox store access and directory access functions are being moved out to the ''middle tier.'' The middle tier is a software/service layer that is designed to sit between the client and the actual data source.

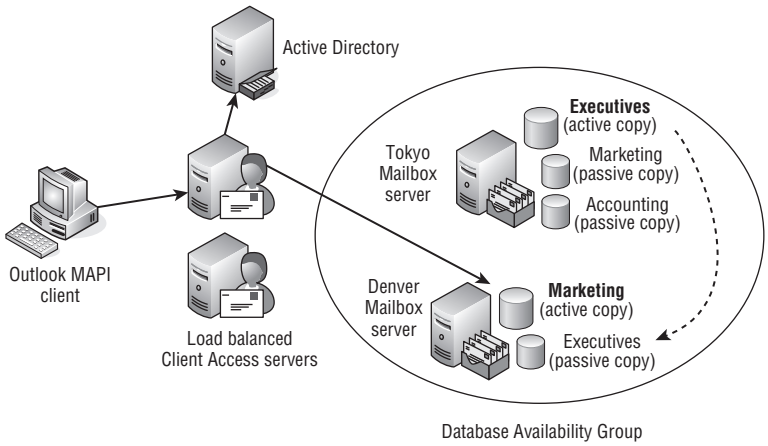
Abstracting the directory referrals or directory access out of the System Attendant is called the Address Book Service (or sometimes called *directory* on the middle tier) while abstracting the MAPI access layer out is called the RPC Client Access Service (or sometimes called *MAPI* on the middle tier). These abstracted functions are now part of the Exchange Server 2010 Client Access server role. Figure 1.8 shows an example of how this might work. A user whose mailbox database is on the Marketing database opens Outlook. For directory and mailbox database access, Outlook connects to a Client Access server. The Client Access server acts as the endpoint for Outlook global address lookups. This is a change from previous versions of Exchange where the server might provide the Outlook client with a referral to the nearest global catalog server. In Figure 1.8, the Client Access servers are load balanced for redundancy.

The Microsoft Exchange RPC Client Access service then looks up the Exchange server on which the user's mailbox database (the Marketing database in this case) is active and proxies MAPI requests for mail data to that server. If the mailbox database is in a DAG and fails over to another server, the connection will automatically be established with the new active server.

One Outlook client connectivity component that remains the same in Exchange Server 2010 is public folder server connectivity. Outlook continues to connect directly to the Exchange

Mailbox server on which a public folder replica is located. The RPC Client Access Service does not handle connectivity for public folders.

FIGURE 1.8
A client using MAPI on the middle tier



Content Storage Improvements

As we mentioned earlier, email systems have evolved not only in their complexity but also in the complexity (and size!) of the messages and mailbox content being sent and stored. Users' demands for improved searching and indexing of their mailboxes have stretched the limits of most server hardware. The following list includes some of the improvements with respect to data storage and recoverability:

- Support for recovering moved or deleted mailboxes using a recovery storage group
- Volume Shadow Copy restoration to recovery databases on alternate servers
- Lost log resilience that allows a database to be recovered even if the last few log files are missing and a new underlying technology that allows for incremental resynchronization

MAILBOX DATABASES

Even in a small or medium-sized organization, mailbox-size constraints are often based solely on the ability to restore a certain amount of data given a specified maximum amount of time. To scale to larger mailboxes, the administrator must create more mailbox stores. While in Exchange Server 2003 Enterprise Edition administrators could create 20 mailbox database spread across four storage groups, Exchange Server 2010 changes this paradigm by not only removing storage groups but also by increasing the number of databases available. The Exchange 2000/2003 term mailbox store has been replaced simply with the term mailbox database.

To allow a server to scale to support larger mailbox sizes or more mailboxes, Exchange Server 2010 Enterprise Edition allows up to 100 mailbox databases of up to 16 TB each. Exchange Server 2010 Standard Edition supports a maximum of five databases of up to 16 TB each.

MAXIMUM NUMBER OF DATABASES AND DATABASE AVAILABILITY GROUPS

Exchange Server 2010 Standard Edition permits a maximum of five mailbox databases on each Mailbox server. Exchange Server 2010 Enterprise Edition permits a maximum of 100 mailbox databases per Mailbox server. The maximum number of mailbox databases includes both the active and the passive copies. You must take this into consideration when planning database availability groups.

SMALLER TRANSACTION LOGS

Experienced Exchange 2000/2003 administrators will immediately recognize an Exchange transaction log because they are always 5,120 KB in size. Exchange 2010 transaction logs, however, are a bit smaller. In fact, the transaction log files are quite a bit smaller — 1,024 KB to be exact.

The transaction log files are smaller because Exchange 2010 includes continuous replication, which allows log files to be copied to another location and replayed into a backup copy of their corresponding database. Reducing the log file sizes ensures that data is copied more quickly to the target.

IMPROVED SEARCH FEATURES

Content indexing has been completely rewritten in Exchange 2010 so that it is far more efficient than in previous versions and is more closely integrated with the Information Store service. Improvements have been made so that the indexing process is throttled back during peak loads and does not affect client use of the Exchange server. By default, each mailbox database automatically has a full-text index associated with it. Messages are indexed upon arrival rather than on a fixed schedule; the index is up-to-date and immediately available to clients.

Full-text search capabilities are available from both Outlook clients as well as Outlook Web App and Windows Mobile devices. Searches can be done by word, phrase, or sentence, and in addition to the message bodies, attachments such as Word documents, Excel spreadsheets, text files, and HTML files can be searched. Where previously the content index could consume between 20 and 40 percent of the size of the database, Exchange Server 2010 content indexing (enabled by default) usually consumes between 5 and 10 percent of the total size of the mailbox database.

Exchange Server Management

Server management with Exchange 2010 becomes increasingly complex as administrators try to make Exchange work within their organizations, particularly in larger organizations. Exchange 2000/2003 management of mail recipients was performed through the Active Directory Users and Computers console, while management of Exchange Server–related tasks and global recipient tasks is performed through the Exchange System Manager console. In Exchange 2010, all recipient administration tasks are now performed through the Exchange Management Console (EMC) or the EMS.

With previous versions of Exchange Server, such as 5.5, 2000, or 2003, medium-sized and large organizations often had specific needs to perform bulk changes to Exchange data, manage Exchange servers from the command line or scripts, and access or manipulate data stored in Exchange databases. Although making bulk changes or manipulating Exchange servers might seem like a simple task (after all, Windows, Active Directory, and Exchange Server are

all from the same company), the truth of the matter is that these tasks were not that simple to perform via script. That has all changed with Exchange Server 2010 (and also with Exchange Server 2007).

Bulk recipient tasks, such as creating multiple mailboxes, changing many email addresses, and configuring bulk properties, can be performed through an application programming interface (API) or scripting interface such as Active Directory Services Interface (ADSI). However, the EMS provides a vastly simpler way to manage all Exchange Server and email recipient properties.

Manipulation of Exchange Server operations, such as mounting and dismounting of databases, queue management, diagnostics logging, and tracking log management, should be handled through the EMS interface.

Finally, accessing or manipulating data stored in an Exchange database is also more complex than it might seem. A popular tool for Exchange 2003 administrators was the Exchange Merge (ExMerge) tool that allowed data to be exported out of an Exchange mailbox and into a personal store (PST) file. Exchange Server 2010 can still use ExMerge, but it can only be used from a client that has the Exchange 2003 administrative tools installed on it. Exchange Server 2007 SP1 introduced a new EMS function that allows the import and export of mailbox data to a PST file via the command line; this feature is also available in Exchange Server 2010, but it does require the x64 version of Outlook 2010.

Clearly, for any organization that is interested in customized management of Exchange (small, medium-sized, or large organizations), Exchange 2003 and earlier versions left a lot to be desired, and required tasks could often not even be performed because of their difficulty. In the minds of many experienced Exchange administrators, this is a gaping hole in the Exchange management architecture.

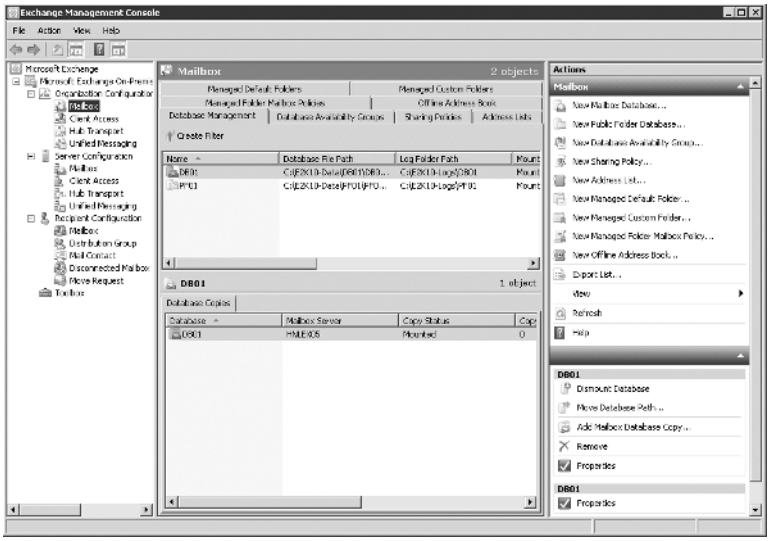


FIGURE 1.9
The new and improved EMC

With Exchange 2010, the management interface has been completely rewritten from the ground up. All management operations related to Exchange management — whether they are performed against an Exchange server, Active Directory, the Registry, or the Internet Information Server (IIS) metabase — have been broken up into unique tasks. All Exchange

tasks can be performed from the EMS (command-line interface); a subset of these tasks can be performed from the EMC graphical user interface. Anything that can be performed from the EMC can be performed via the EMS; there are advanced administrative tasks that can be performed only from the EMS.

The EMC (shown in Figure 1.9) has been completely redesigned to make it easier to use, to better organize Exchange management tasks, to reduce the complexity, and to make administrative tasks more discoverable.

The new console is built on top of an entirely new scripting technology called PowerShell and a set of Exchange-specific extensions called the EMS.

Improved Message and Content Control

All messaging system administrators can relate to challenges, such as adequately managing the content that is stored on their mail servers, keeping business-essential information available when it is required, removing content that is no longer necessary, controlling the flow of messaging information, and preventing disclosure of information. If one or more of these challenges has been a problem for you, then Exchange 2010 has solutions.

Messaging Records Management

Messaging records management was initially introduced in Exchange Server 2007and brings about a new concept in the control of messaging content. Messaging records management allows administrators to more closely control the life of message content (email, voicemail, calendar entries, and so on) from the moment the information is created on the Exchange server until the point at which that information no longer has business or legal value. This helps the organization maintain important records as long as necessary but discard unnecessary information in a timely fashion. These are configured at the organization level so they will affect all Mailbox server roles.

To a certain extent, some of the features of messaging records management are distantly related to the Exchange 2000/2003 Mailbox Manager. There are a number of components to messaging records management, as shown in Table 1.2.

TABLE 1.2: Messaging records management features

COMPONENT	FUNCTION
Managed default folders	Default folders are found when an Outlook MAPI client uses its mailbox, including Calendar, Contacts, Deleted Items, Inbox, Junk E-mail, Sent Items, RSS Feeds, and so on.
Managed custom folders	Managed custom folders are folders that are created by the Exchange server administrator for users who are included in a managed folder mailbox policy. Storage limits and managed content settings can be applied to these folders.
Managed folder mailbox policies	Managed folder policies define which folders are included in a particular policy. Managed folder mailbox policies are then assigned to mailboxes.
Managed content settings	Managed content settings define retention settings and message journaling features for content, such as messages and voicemail.

Once a user has been assigned to a managed folder mailbox policy, any additional custom folders that must be created in that user's mailbox will show up in the Managed Folders folder in the root of the user's mailbox, such as those shown in Figure 1.10. You can now configure message journaling based on a specific type of content or folder.

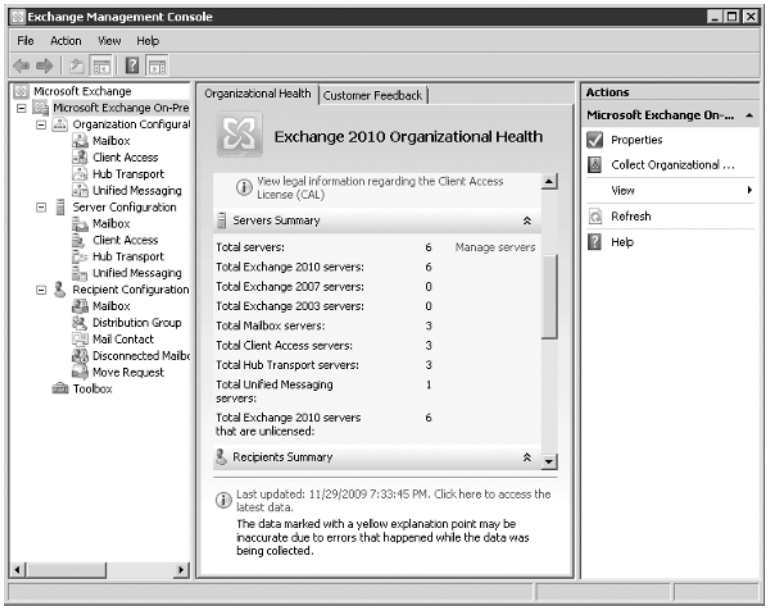


FIGURE 1.10
Managed folders assigned by the managed folder mailbox policy

Normally, content in these folders will be managed by the end user. Moving relevant content into these folders is their responsibility. In certain situations, a user can specify managed content settings that can accurately identify content types such as messages or voicemail and can move them into the appropriate custom-managed folders. A user can also build client-side rules that move content into their managed folders. Let's take a quick look at some of things that you can do with messaging records management:

- Control the length of time and the content types in users' folders.
- Define additional folders that should be created in a user's folder that the user can use for message retention. Differing retention policies can be defined for the custom folders that you create for your users.
- Automatically send copies of messages that users place in a managed folder to another email address each time the managed mailbox assistant runs.
- Move messages from a specified folder based on content type (email, contact, calendar, voicemail, etc.) to another managed folder.

The first time you look at messaging records management, it is a bit confusing until you realize that it must be configured in a few different steps, such as the following:

- Create managed folder mailbox policies to define which managed default and managed custom folders will be managed.

- Assign the managed folder mailbox policy to one or more users. A user does not need a managed folder mailbox policy. Only a single managed folder mailbox policy can be assigned to a user at one time.
- Create managed content settings for default folders (Inbox, Sent Items, etc.) to control the length of time that messages should remain in these folders and types of content that are allowed. This step is optional.
- Create managed custom folders that will appear in the user's Managed Folders folder in their mailbox. This step is optional.
- Create managed content settings for managed custom folders to control how content is managed or retained in the folders that will be created in the user's mailbox. This step is optional.

One confusing point with respect to messaging records management is that on the surface it is documented as a premium feature of Exchange 2010 and thus requires an Enterprise Client Access License for each user who will have their mailbox managed by it. However, Microsoft makes an exception if you are using messaging records management features to simply clean up message items in the folders in the same way you would have used the Exchange 2000/2003 mailbox management feature.

Built-In Archiving

The market for third-party tools to support Exchange Server has grown rapidly since the release of Exchange Server 2003. At one point, there were more than 60 third parties providing email archive solutions for Exchange Server. The sheer volume of email that users receive and the users' demand that they be able to keep their historical email has made these tools very attractive.

Exchange Server 2010 introduces a new premium feature that allows for the integration of email archiving. The email archiving feature is actually a series of features that interact directly with the user's mailbox:

Archive Mailbox Defined on a user-by-user basis since all users might not need an archive mailbox. The content in the archive mailbox can be accessed by users using the Outlook 2010 client or Outlook Web App 2010.

Retention Policies Define the types of mail and how long the mail can be retained within the user's primary mailbox. Retention policies can be defined that control when items are permanently deleted or when they are moved in to the archive mailbox. With Outlook 2010, end users can participate in the retention process by applying retention tags to messages or an entire folder.

Multi-mailbox Search Allows an authorized user to search for content across multiple mailboxes (both the user's ''active'' mailbox as well as their ''personal archive mailbox'') within an organization. This would be useful during a lawsuit and an electronic discovery action became necessary.

Legal Hold Allows the administrator to place a ''hold'' on a user's mailbox so that deleted and edited items are held during the hold period. This would be necessary in the event of legal action or an investigation regarding the conduct of one or more of your users.

Ultimately, the new Exchange 2010 archiving and retention policies are intended to replace the messaging records management features that were introduced in Exchange Server 2007.

More information on the archive and retention policy features can be found in Chapter 22, ''Getting Started with Email Archiving.''

Message Transport Rules

Message transport rules are quite similar to Outlook rules and are even created using a wizard similar to one used to create Outlook rules. However, these rules are quite a bit more powerful and are executed on the Hub Transport servers. Since all messages are processed by a Hub Transport server whether they are inbound, outbound, or for local delivery, you can build powerful policies to control the messages and data that flows within your organization. Transport rules can also be defined at your organization's perimeter by using an Edge Transport server.

Although we will cover a lot more about transport rules in Chapter 26, ''Managing Transport and Journaling Rules,'' just to give you a taste of what you can do with transport rules, it is useful to highlight some of the cool things you can do with them:

- Append disclaimers to outgoing messages
- Implement message journaling based on recipients, distribution lists, message classification, or message importance
- Prevent users or departments from sending email to another by creating an ethical wall (a.k.a. a Chinese wall)
- Intercept messages based on content or text patterns using regular expressions (REGEX) found in the message subject or message body
- Apply message classifications to messages based on sender or message content
- Take action on a message with a certain attachment or attachment type or an attachment size that exceeds a specified limit
- Examine and set message headers or remove data from the message header
- Redirect, drop, or bounce messages based on certain criteria
- Apply Microsoft Rights Management Service (RMS) encryption-based transport rule conditions

Every transport rule has three components: conditions, actions, and exceptions. The conditions specify under what conditions the rule applies whereas the exceptions specify under what conditions it will not apply. The actions are the interesting part of the transport rule. Figure 1.11 shows the Conditions page of the Transport Rule wizard; this screen has two parts. The first part is simply checking the actions to take, and the second part specifies more details about the action.

For the transport rule you see in Figure 1.11, previously on the Conditions page, we selected a condition From People in Step 1, but in Step 2, we have to specify the list of people (or groups). In this case, we selected the group VIPs. On the Actions page (shown in Figure 1.11), we selected the Log An Event With Message, Apply Message Classification, and Blink Carbon Copy (BCC) The Message To Addresses options.

In the Step 2 box, we then have to specify the text of the event to log, the classification to apply, and to whom the BCC message should be sent.

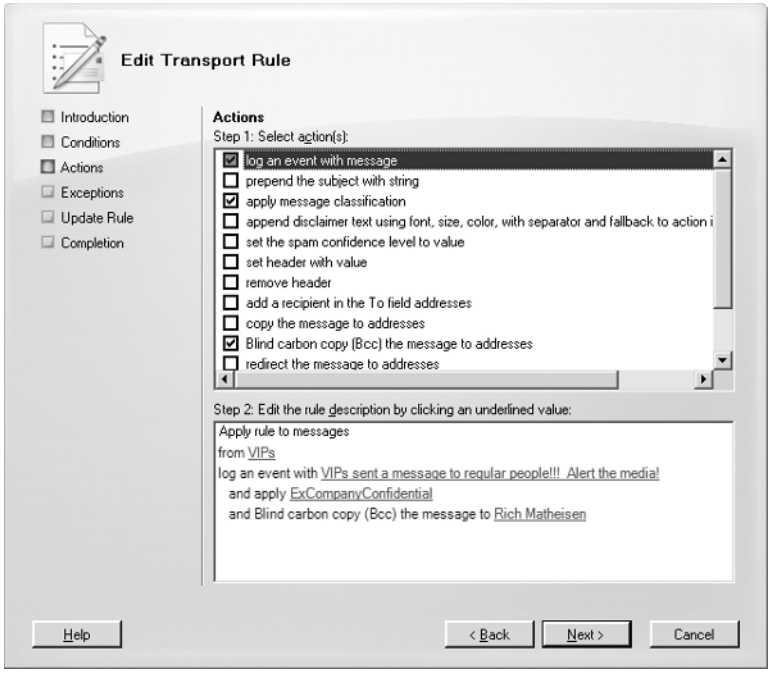


FIGURE 1.11
Examining a transport rule

Per-User Journaling

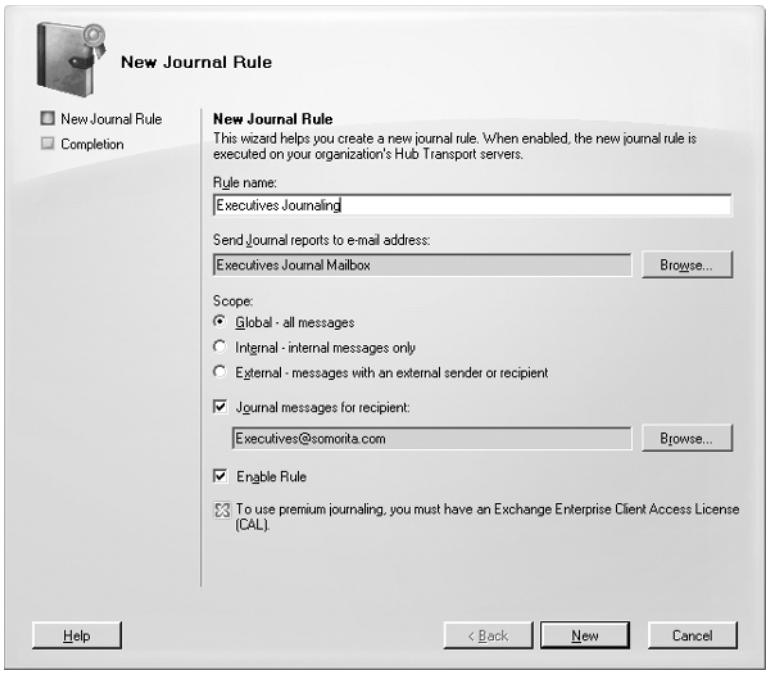
Journaling a message is the process of keeping a message from one or more senders based on long-term storage, legal, regulatory, or human resources requirements. Exchange 2000/2003 essentially had one option for message journaling: create an additional mailbox store and move any mailboxes that must be kept to that mailbox store. Note that a true journaling solution happens before the user has any input into the process; a message is intercepted prior to or at the time of delivery via transport rules or by rules set on the mailbox database. A true message journaling feature produces a message envelope header that exposes the sender and recipient information as well as containing the original message. Exchange 2010 has many new options with respect to retaining messages; however, only the first two are considered true message journaling features:

- Messages can still be retained based on the journal settings on the mailbox database.
- Messages can be retained using a new hub transport feature called a journaling rule that allows messages to be retained based on a single sender or distribution group membership.
- Messages can be retained based on folder or content type using managed content settings; note that this is not considered true journaling because it is merely moving mail from one folder to another after the fact.
- Messages can be retained using transport rules by examining sender, recipient, message priority, message classification, or message content. This solution does not create a true journaling message.

- Messages can also be retained using transport rules by keeping only internal or only external messages.
- Messages can be sent to an SMTP address that is external to the Exchange organization, such as a Microsoft Office SharePoint Server 2007 server or a third-party service provider.

Figure 1.12 shows an example of a transport rule that applies to the Executives group. Any mail sent to members of the Executives group has a copy of that message sent to the Executives Journal Mailbox. While the journal rule shown in Figure 1.11 shows an internal Exchange mailbox in the Send Journal Reports To E-mail Address box, this could be any valid mail-enabled recipient (such as a mailbox-enabled user, mail-enabled user, or mail-enabled contact).

FIGURE 1.12
Creating a journaling rule



Journaling is a premium feature and thus requires an Exchange Server 2010 Enterprise Client Access License for each user who will have their mail journaled.

Message Classifications

Organizations that send confidential, proprietary, or classified information via email often implement message classification templates. However, these client-side templates display the message classification only for the sender and the recipients; in previous versions of Exchange there was nothing within the message transport that could take action on or evaluate a classified message.

Exchange 2010 allows a message to enforce rules based on the classification of a message, such as Do Not Forward, Partner Mail, Attachment Removed, Company Confidential, Company Internal, Attorney/Client Privilege, and customized classification levels. The sender can assign the classification using Outlook 2007, Outlook 2010, or Outlook Web App 2010, or

message transport rules can assign a classification based on sender, recipient, message content, importance, and so on. Figure 1.13 shows an example of a message that is being composed in Outlook Web App and has had the built-in Attorney/Client Privilege classification assigned to it; the classification text is shown just above the address list. The server administrator can create additional classifications and customize the text strings.

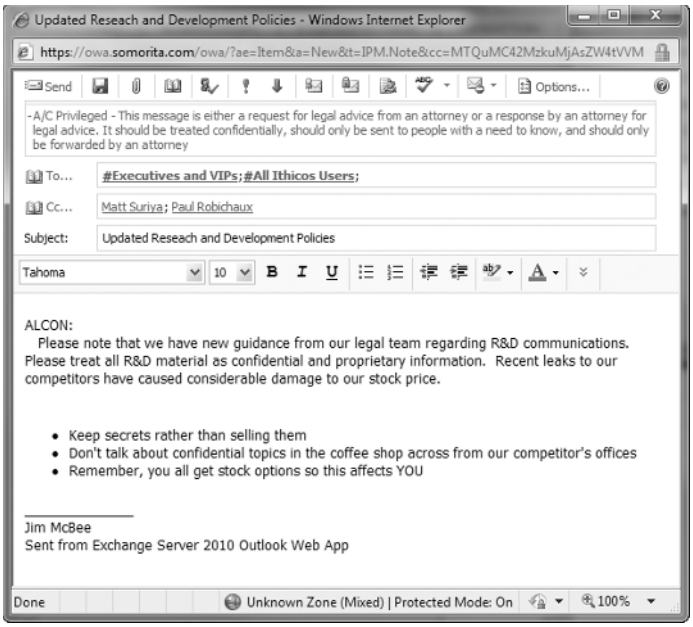


FIGURE 1.13
Classifying a message using Outlook Web App

Rights Management Service Message Protection

If you are concerned about message content protection, one of the cool new features of Exchange Server 2010 is its integration with the Microsoft Active Directory Rights Management Services (RMS). While RMS has been integrated with the Outlook client for quite a few years now, Exchange Server 2010 introduces significantly better integration. Features include the following:

- Hub Transport server transport rules can now apply rights management protection to messages and attachments based on rule conditions.
- The Hub Transport service can be configured to allow decryption of information rights management (IRM) protected messages in transit in order to apply messages policies to the message.
- IRM provides protection for Unified Messaging voicemail messages.
- IRM protection is now integrated with Outlook Web App 2010.

New Programming Interfaces

Much of the underlying infrastructure of Exchange 2010 has been completely rewritten since Exchange Server 2000/2003. As a result, many of the APIs used to access Exchange data and to manage Exchange components have been replaced with new APIs.

EXCHANGE MANAGEMENT

Management of Exchange-related components and recipient objects is now performed with the new management API. All operations that can be performed have been defined as tasks. The management API provides access to all management functions via the EMS tasks, also known as cmdlets (pronounced ''command-lets''). The EMS is a set of extensions for the Windows PowerShell. Exchange management functionality can be extended and accessed via managed code, and custom scripts can integrate with and use .NET objects.

TRANSPORT AGENTS

All messages and message content traveling through the message transport system (on a Hub Transport server or Edge Transport server) can be manipulated using transport agents. Transport agents are written using managed code. They replace Exchange 2000/2003 transport sinks.

EXCHANGE-MANAGED APIS

Exchange-Managed APIs extend the Microsoft .NET Framework by providing classes and data structures that allow custom programs to access and manipulate different parts of email message content. Functions include accessing MIME content; filtering email body content; converting message content between plaintext, HTML, and RTF formats; and reading or writing calendar items.

WEB SERVICES

One of the most exciting new APIs is the Web Services API. Using Web Services, developers can write applications that can remotely access mailboxes, folders, and message content. Many of the new Exchange services — such as the Autodiscover service, Availability service, and messaging records management — use the Web Services API. Services can be developed that can send notifications to client applications and provide synchronization of mailbox folders and items. The Web Services API provides these features:

- Ability to manage folders in a user mailbox, including creating, deleting, copying, changing, searching, viewing, and moving folders
- Ability to manage messages in a user mailbox, including creating, deleting, copying, changing, searching, viewing, moving, and sending messages as well as accessing message content
- Ability to enumerate distribution group memberships

Client-Side Features

There are a number of improvements that in Exchange Server 2010 that will directly affect the end user. These are improvements that did not exist in Exchange Server 2000/2003.

Schedulable and Internal/External Out-of-Office Messages

A very nice improvement from the user's perspective is the ability to schedule when out-of-office messages start and finish and the ability to specify a separate message for internal users than you have for external users. For this feature to work properly, you need either Outlook Web App 2010 or Outlook 2007/2010. Figure 1.14 shows an example of the Out Of Office Assistant in Outlook Web App.

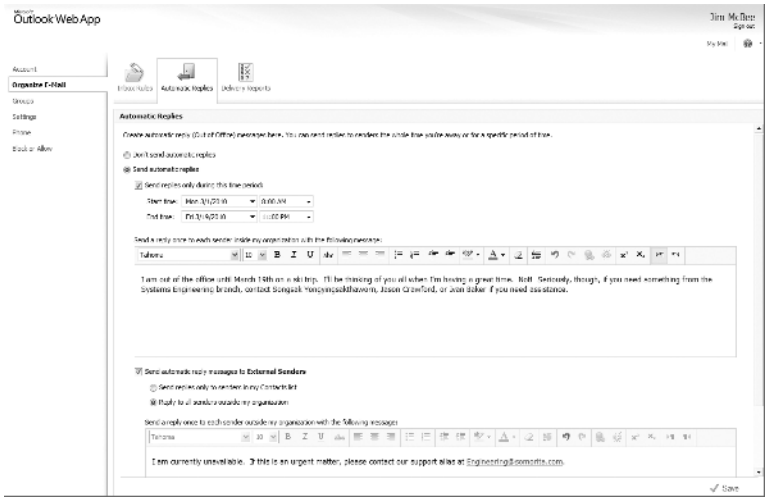


FIGURE 1.14
Scheduling out-of-office messages for internal and external recipients

When setting up an out-of-office message for external recipients, the user can specify that the response go only to senders whose address is in their Contacts folder or to any sender.

Improved Calendaring and Resource Management

Calendaring, resources, and out-of-office features were not as complete as most of today's sophisticated email users require. Exchange 2010 and Outlook 2007 have improved each of these with new features and functions. For many of the calendaring and resource management features to work properly, Outlook 2007 or later or Outlook Web App 2010 is required. The Availability service now works between multiple Exchange Server 2010 organizations provided the cross-organization features are enabled.

Resource Management

One of the biggest hurdles that messaging system managers have had to overcome with Exchange is how to manage resource calendars. In earlier versions of Exchange, a resource calendar was nothing more than a mailbox whose calendar was shared with other users or a mailbox that had scripts or event sinks that allowed for automatic acceptance and processing of meeting requests for a particular resource. Exchange 2010 improves on the concept of resource mailboxes. At mailbox creation time (see Figure 1.15), the administrator designates the type of resource that is being created (room or equipment).

Administrators can then set custom properties, such as room capacity or audiovisual capabilities, for this resource. This information can be viewed within Outlook 2007/2010 when a user is looking for a resource that suits the user's requirements. The Resource Booking attendant provides features that control who can book a resource, for how long, and during which hours, and it also provides conflict information.

Calendar Concierge

As users have become more sophisticated, their calendaring requirements have increased. The Calendar Concierge is a collection of features that allow for better management of user and resource mailboxes. The Exchange 2010 Calendar Assistant helps to keep out-of-date meeting requests from disturbing the user by ensuring that they are presented with only the most recent meeting request. The Calendar Assistant also reduces the amount of unnecessary messages

relating to meeting requests, such as a Tentative response followed soon after by a Decline or Accept response. The user sees only the most recent message.

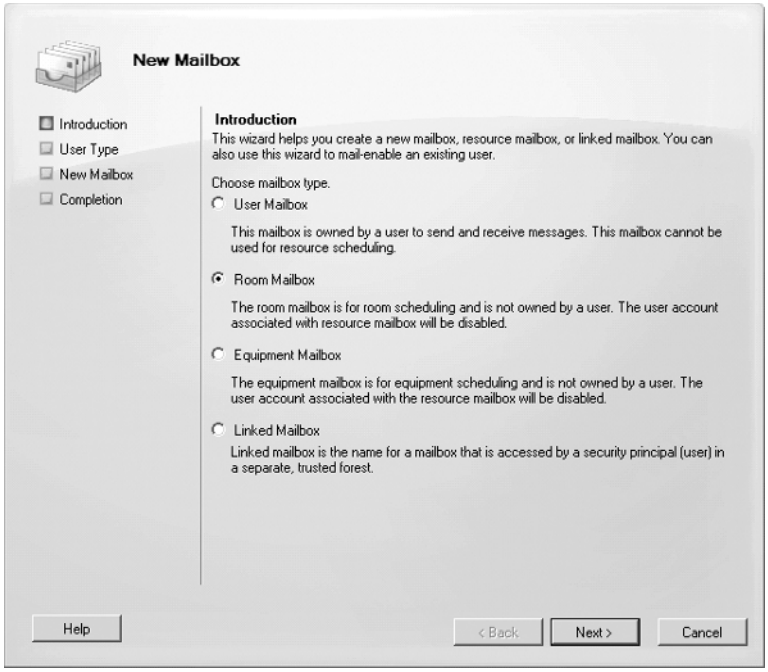


FIGURE 1.15
Resource type is designated when the mailbox is created.

The Scheduling Assistant makes the process of scheduling a meeting using either Outlook or Outlook Web App much simpler and recommends best meeting times based on requested attendees.

AVAILABILITY SERVICE

Earlier versions of Exchange used a system public folder for publishing a user's free/busy information. Periodically, the Outlook client had to connect to this public folder and update the user's free/busy times. Exchange 2010 supports a new Web Service that runs on the Client Access server role and provides an interface to all users' free and busy times. Outlook 2007/2010, the Outlook Web App 2010, and Entourage clients are able to use this new Web Service, so the Availability service ensures that free and busy times published by older clients are accessible via the Web Service and free and busy times published by Outlook 2007 and later are available via the system public folder.

AUTODISCOVER

One of the most time-consuming things that an Exchange administrator has to do is to help configure Outlook clients to connect to the Exchange server. In the past, profiles had to be created via scripting or profile utilities. Exchange 2010 introduces a feature called Autodiscover that makes configuration of Outlook 2007 (or later) profiles much simpler. Once the user provides their name and their email address, Outlook 2007 (or later) automatically discovers the correct server and updates the server if the mailbox moves (even if the original server is no longer online).

New and Improved Outlook Web App

Those of us who gushed when we saw the Outlook Web Access interface in Exchange 2003 thought a web interface could not get much better. For Outlook Web App in Exchange 2010, the Exchange team started over from scratch to build a much more functional interface than ever before. Here are some of the new features in Outlook Web App 2010:

- Ability to browse the Global Address List (GAL)
- Ability to manage and remotely wipe Windows mobile devices
- Improved meeting booking features
- Ability to perform full-text searches on mailbox content
- Selectable message format (HTML or plaintext) when composing a message
- Ability to set out-of-office messages, define them as internal or external, and schedule when they start
- Ability to manage voicemail features such as their greeting, reset their voicemail PIN, and turn on missed call notifications
- Conversation view, which provides threaded views of email conversations
- Exchange Control Panel (ECP), which allows an end user to update their own directory information as well as manage their own group membership

Windows Mobile and Improved Security

Windows Mobile and ActiveSync device support are certainly not new features to Exchange Server 2010. Exchange Server 2003 had good support for Windows Mobile devices, and you could even support mobile devices using Microsoft Mobile Information Server and Exchange 2000.

If you have supported Windows Mobile devices or other types of mobile devices, you realize how important centralized policies and security can be for your organization and your users. The latest versions of Exchange ActiveSync (EAS) have been improved greatly over the years. The newest features can be assigned to users based on the ActiveSync policy that is assigned to the user. Figure 1.16 shows two of the advanced properties pages.

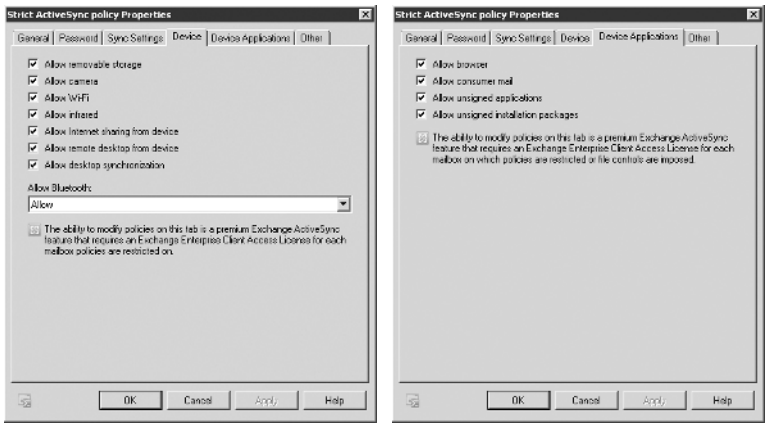


FIGURE 1.16
Examples of ActiveSync policies

Of course, you have to have the corresponding version of Windows Mobile that will take advantage of all the newest features. Windows Mobile 5 with the Microsoft Security and Feature Pack (MSFP) uses EAS v2.5, Windows Mobile 6 uses EAS v12, and Windows Mobile 6.1 uses EAS v12.1. Table 1.3 shows a comparison of some features of various versions of EAS and the versions of Exchange Server.

TABLE 1.3: Exchange ActiveSync Features

SETTING/RESTRICTION	E2K3 SP2 EAS v2.5	E2K10 EAS 12	E2K10 STANDARD CAL EAS v12.1	E2K10 ENTERPRISE CAL EAS v12.1
Password Required	✓	✓	✓	✓
Min Password Length	✓	✓	✓	✓
Alphanumeric Pwd	✓	✓	✓	✓
Inactivity Timeout	✓	✓	✓	✓
Max Failed Password Attempts	✓	✓	✓	✓
Policy Refresh Interval	✓	✓	✓	✓
Allow Non-provisionable Devices	✓	✓	✓	✓
Attachments Enabled		✓	✓	✓
Storage Card Encryption		✓	✓	✓
Password Recovery Enabled		✓	✓	✓
Allow Simple Device Password		✓	✓	✓
Max Attachment Size		✓	✓	✓
WSS Access Enabled		✓	✓	✓
UNC Access Enabled		✓	✓	✓
Password Expiration		✓	✓	✓
Password History		✓	✓	✓
Require Manual Sync When Roaming			✓	✓
Min Device Pwd Complex Characters			✓	✓
Max Calendar Age Filter			✓	✓
Allow HTML Email			✓	✓
Max Email Age Filter			✓	✓
Max Email Body Truncation Size			✓	✓

TABLE 1.3: Exchange ActiveSync Features *(CONTINUED)*

SETTING/RESTRICTION	E2K3 SP2 EAS v2.5	E2K10 EAS 12	E2K10 STANDARD CAL EAS v12.1	E2K10 ENTERPRISE CAL EAS v12.1
Max Email HTML Body Truncation Size			✓	✓
Require Signed SMIME Messages			✓	✓
Require Encrypted SMIME Messages			✓	✓
Require Signed SMIME Algorithm			✓	✓
Require Encryption SMIME Algorithm			✓	✓
Allow SMIME Encryption Algorithm Negotiation			✓	✓
Allow SMIME Soft Certs			✓	✓
Require Device Encryption			✓	✓
Allow Storage Card				✓
Allow Camera				✓
Allow Unsigned Applications				✓
Allow Unsigned Installation Packages				✓
Allow Wi-Fi				✓
Allow Text Messaging				✓
Allow POP/IMAP Email				✓
Allow Bluetooth				✓
Allow IrDA				✓
Allow Desktop Sync				✓
Allow Browser				✓
Allow Consumer Email				✓
Allow Remote Desktop				✓
Allow Internet Sharing				✓
Unapproved InROM Application List				✓
Approved Application List				✓

Note that some of the advanced device configuration features require the use of an Exchange Server 2010 Enterprise Client Access License (CAL) for the device. This does not mean that the Exchange 2010 server requires the Enterprise Edition of Exchange Server, though.

Now, Where Did That Go?

As new and better functions and APIs have been introduced, naturally some functions are no longer emphasized or supported. There has been a lot of confusion surrounding what will continue to be supported in Exchange 2010 and what will no longer work. The phrase ''no longer supported'' itself tends to also generate a lot of confusion because a function may actually continue to work because it has not truly been removed. These functions and APIs fall into two unique categories: functions that have been deemphasized and functions that are no longer available.

Deemphasized Functions

When Microsoft says that in Exchange 2010 certain functions or APIs are no longer emphasized, this means that the company will not continue to enhance these features. The features will continue to be supported, and if there are bugs with these features, the bugs will be fixed. However, if something is being deemphasized, the writing is on the wall; you should consider replacing your use of this technology with something else.

The following is a list of some of the APIs and functions that are being deemphasized:

- Public folders are still supported in Exchange 2010, but their use is being deemphasized as newer collaborative technologies have been introduced, such as SharePoint and other portal technologies.
- Collaborative Data Objects technologies such as CDOSYS, CDO 1.2.1, and CDOEXM have been removed completely. Applications using these APIs should be rewritten using the Transport Agents API or Exchange Web Services API.
- Functions provided by Exchange WebDAV extensions are now provided by the Web Services API. If you have applications that require WebDAV, you will have to either update them or keep an Exchange 2003/2007 server running.
- The Exchange Object Linking and Embedding Database (ExOLEDB) API functionality is now provided via the Web Services API.
- Store events were removed from Exchange Server 2010 and should be replaced with functions written using the Web Services API.

Features No Longer Included

As Exchange Server has evolved into its current form, the code has experienced significant changes. This includes many of the new features we have discussed in this chapter, but there have also been features and programming interfaces that have been removed because it just no longer makes sense to support outdated technologies.

Some features and APIs have been completely removed from the Exchange 2010 product. If you require any of these features or APIs, you may need to keep an Exchange 2003 server in operation. If you still require features provided by the Exchange 2000 Server platform, you are not even going to be able to transition to Exchange Server 2010 until you can replace that particular feature requirement with newer software.

Exchange Server 2003 Features Removed from Exchange Server 2010

Since the release of Exchange Server 2003, a number of Exchange Server 2003 (and Exchange 2000) features have been removed. Although most of these features will not affect the majority of the Exchange deployments out there, you should keep them in mind and thoroughly evaluate your existing messaging environment to make sure you are not dependent on a feature that has no equivalent in Exchange Server 2010. Here are some of the Exchange Server 2003 features and functionality that have been removed from the product:

- Exchange 5.5 and Exchange Server 2000 interoperability is no longer available and there is no transition path between these legacy versions and Exchange Server 2010. You cannot install an Exchange 2010 server until your Exchange organization is in native Exchange mode.
- Outlook Mobile Access, the lightweight browser-based access for WAP-based mobile phones, is not available. Nor are Exchange ActiveSync Always Up-to-Date notifications.
- Non-MAPI public folder hierarchies are no longer available.
- Public folder access via NNTP and IMAP4 is no longer available.
- Network News Transport Protocol (NNTP) features have been cut from Exchange 2010 completely.
- Routing groups and routing group connectors are no longer required once you have completely migrated to Exchange Server 2010. In a native Exchange 2010 organization, the message routing topology is determined using the Active Directory sites in which the Exchange servers are located. Message delivery between Exchange 2010 servers in different Active Directory sites is handled automatically.
- Mailbox databases no longer have a streaming database file (STM file). All mail, regardless of its original source, is stored in the EDB database file.
- The Recipient Update Service functionality has been replaced. Email proxy addresses and address list membership is set on a mail recipient object at the time of creation. They can be updated from the EMS.
- X.400 connectors are no longer available.
- ExMerge can no longer be run from the Exchange 2010 server console; it can continue to be run against Exchange 2007 mailboxes, but it must be run from a computer with Outlook installed.
- Mail recipient management using the Active Directory Users and Computers console extensions no longer works. All recipient management must be performed through the EMC. A few exceptions exist, of course, but using the EMC or the EMS is preferred. This will also keep you from accidentally doing something that is not supported.
- Administrative groups are no longer available. All permissions delegation is handled via either a series of built-in groups or via the new role-based authorization control (RBAC) feature.
- Development APIs and tools, such as CDO v1.2, CDO for Workflow, CDOEXM, Exchange WMI classes, Exchange Web Forms, Workflow Designer, ExOLEDB, store events, and transport event sinks, are no longer available.

- The Exchange installable file system (ExIFS), which was also known as the M:\ drive, is no longer available.
- The GroupWise, cc:Mail, and Microsoft Mail connectors are no longer available.

Exchange Server 2007 Features Removed from Exchange 2010

Although Exchange Server 2007 did not enjoy wide deployment, there will be organizations that will be transitioning from Exchange Server 2007 to Exchange Server 2010. A number of features have been removed from Exchange since Exchange Server 2007; this list is in addition to the features that were removed since Exchange Server 2003. The following Exchange Server 2007 features are no longer available:

- Local Continuous Replication (LCR)
- Single Copy Clustering (SCC)
- Cluster Continuous Replication (CCR)
- Standby Continuous Replication (SCR)
- Unified Messaging inbound faxing functions
- Streaming backups
- SharePoint document library and network share access via Outlook Web Access
- 32-bit management tools

Clearing Up Some Confusion

We mentioned earlier that Exchange has certainly been hyped a lot during the design and beta-testing process. This has generated a lot of buzz in the information technology (IT) industry, but this buzz has also generated a lot of confusion and some misinformation. We want to take this opportunity to clear up some of this confusion by answering a few of the common questions that have generated misconceptions about Exchange 2010.

Do I have to have three or four separate servers to run each of the server roles? In a small environment, a single server can host all four primary server roles (Mailbox, Client Access, Hub Transport, and Unified Messaging), though Microsoft recommends against hosting the Unified Messaging role on the same server. Unlike Exchange Server 2007, an Exchange 2010 server can host the Mailbox, Client Access, Hub Transport, and Unified Messaging roles. The Edge Transport role must be installed on a separate server.

Is there a 32-bit version of Exchange? No, no 32-bit version of Exchange 2010 is available.

Is the Edge Transport server required? No, Edge Transport servers are not required. You can use any third-party message hygiene system in your perimeter network, or you can direct inbound and outbound mail through your Hub Transport servers, or both.

Does Exchange 2010 use a SQL database for mailboxes and public folders? Although there has been debate for years about using SQL Server for the Exchange databases, Exchange 2010 uses the Extensible Storage Engine (ESE), also known as the JET database engine.

Is EMS knowledge required? Do I have to learn scripting? Most common administrative tasks can be performed through the EMC graphical interface. Command-line management and

scripting for Exchange 2010 has been greatly improved through the use of the EMS. Many tasks are simplified or more powerful through the EMS, but it is not necessary to learn scripting in order to start working with Exchange 2010. We strongly encourage you to get to know many of the powerful features of the EMS as you get comfortable with Exchange 2010. A number of advanced administration tasks do not have a graphical user interface option.

What is happening with public folders? The use of public folders with Exchange 2010 is still available and supported, but their use is being deemphasized as newer collaborative technologies such as websites and portals have become commonplace. We urge you to examine your public folder applications with an eye toward migrating them to systems such as Microsoft Office SharePoint Server 2007.

Is there still a 32 KB limitation on folder rules? For power users, the 32 KB limit on the size of rules for a folder was a serious annoyance. This limit is no longer a constraint for users whose mailbox is on an Exchange 2010 mailbox server.

Do I need to use every Exchange 2010 server role to have a functional Exchange 2007 system? To build a completely functional Exchange 2010 system, you need the Mailbox, Hub Transport, and Client Access server roles.

Can I run 32-bit applications with the 64-bit version of Exchange 2010? Most 32-bit Windows applications will generally run on Windows 2008 x64, but applications that integrate with Exchange (such as message hygiene or backup applications) should be 64-bit.

The Bottom Line

Understand new high-availability options. Exchange Server now provides replication technology that keeps databases synchronized between an active copy of the database and one or more passive copies. In the event of failure of the active database, one of the passive copies can be brought online. Storage groups have been eliminated and now each Exchange database has its own set of transaction logs.

An Exchange Mailbox server can belong to a database availability group (DAG). Exchange databases can be synchronized to one or more members of a DAG. Failovers between servers can now be handled at the database layer rather than a single database failure having to cause an entire cluster node to fail over.

> **Master It** You have been asked to provide a high-availability solution for your organization's 1,000 mailboxes. Describe the Exchange Server 2010 feature that will allow you to provide high availability for your Exchange 2010 mailboxes.

Understand new recipient management features. The underlying management components for all Exchange server and mail recipient administration have been completely rewritten from scratch. All management tools are built on top of the Windows PowerShell and are included in the EMS. Exchange administration can now be performed from either a graphical user interface (the EMC) or the EMS. The EMS often includes functions that are not available from the management interface.

> **Master It** You support 8,000 mailboxes in your Exchange Server 2010 organization. You have been asked to perform a management task on mailbox-enabled users in your

organization. This task consists of setting the Outlook Web App policy to a new policy name. What is the quickest way to assign all of your users the new policy?

Recognize Exchange architecture changes. Significant changes were made to the Exchange Server 2010 architecture to improve the scalability, security, and stability. This includes providing only an x64 edition of Exchange Server 2010. Requiring an x64-based operating system and hardware dramatically improves the scalability and performance of Exchange Server 2010. The x64 architecture means that Exchange Server 2010 can now access more than 3 GB of physical memory. Microsoft has tested server configurations with up to 64 GB of physical memory. The additional physical memory means that data can be cached and written to disk more efficiently. This greatly improves the Exchange Server 2010 disk I/O profile over previous versions.

Unlike Exchange Server 2003 and earlier where a server's roles and functions were configured after installation, Exchange Server roles allow the Exchange administrator to define the functions of the server during installation.

Master It You are planning your Exchange Server 2010 infrastructure to provide basic messaging functionality (email, shared calendars, and Windows Mobile phones). Which Exchange Server roles will you need to deploy?